CEA
Advocating for teachers
and public education

Connecticut Education Association

Governance
Sheila Cohen, President
Jeff Leake, Vice President
Pat Jordan, Secretary
Thomas Nicholas, Treasurer
John Horrigan, NEA Director
Gary Peluchette, NEA Director

Executive Office
Mark Waxenberg
Executive Director

Policy, Research & Reform
Dr. Linette Branham, Director
Donald E. Williams, Jr. Deputy Director
Capitol Place, Suite 500
21 Oak Street
Hartford, CT 06106
860-525-5641 800-842-4316
Fax 860-725-6328

An affiliate of the
National Education Association

Ray Rossomando

Connecticut Education Association

Before the

Education Committee

March 19, 2015

Re:

HB 7017 AAC Student Data Privacy

Good afternoon Senator Slossberg, Representative Fleischmann, and members of the Education Committee. My name is Ray Rossomando, Research and Policy Development Specialist for the Connecticut Education Association. CEA represents 43,000 active and retired teachers across the state.

I am testifying today on HB7010, AAC Student Data Privacy. CEA supports the provisions included in this bill, but believes that they do not go far enough in protecting personally identifiable information in this new and increasingly nebulous climate of digital data availability.

There are numerous factors that warrant stronger action on data privacy this year. Our testimony focuses on four:

1) Unprecedented ability to transfer Personally Identifiable Information (PII) in a click of a mouse
2) Misuse of data for purposes detrimental to public education and educators
3) Obliteration of federal data privacy (FERPA) protections and deleting parental consent
4) Data breaches involving PII occur frequently

CEA believes that there are many stronger options that could be included in a bill revising data privacy rules this year, including:

Restore and Improve Education Records Protection – Reverse the US DoE's weakening of FERPA rules by creating stronger state laws that:

- Restore requirements for parental consent before student PII is shared with a third party or other governmental agencies.
- Extend protections to personally identifiable teacher data, particularly data linked to individual students and classroom levels.

- Require contractors with responsibility over educational PII to register with the state and to be subject to a fine of up to $50,000 for violating privacy laws.

Increase Data Use Transparency and Information Available to Parents

- Require parental consent for the sharing of PII and require notification of data uses, data sharing contracts, and parental privacy rights.
- Require the SDE to make public an inventory of data elements it collects.

CEA recommends that this committee look to the work done in Colorado, Idaho, and California for further direction, as well as the work of EducationCounsel.org on this topic. EducationCounsel recently published this helpful look at best practices, state policies, and model legislation: *Key Elements for Strengthening State Laws and Policies Pertaining to Student Data Use, Privacy, and Security: Guidance for State Policymakers*.

For news reports, court cases, analyses of data security issues, and legal analyses, CEA also recommends the Electronic Data Privacy and Information Center (EPIC) https://epic.org/privacy/student/. We hope committee members find this resource useful.

As committee members consider this bill, we urge you to consider the evolving climate that has made data more vulnerable to misuse, abuse, and breach. We specifically draw your attention to the following four concerns and potential solutions to them:

1) Unprecedented ability to transfer PII in a click of a mouse

To begin, PII – whether PII of students, educators, and the public at-large – is becoming increasingly easier to be transferred, uploaded, or otherwise shared or even stolen digitally. As a result, data is more vulnerable today to misuse, and the threats to data security are mounting. In fact, just yesterday former presidential advisor Diane Ravitch posted an ad she received (attached) offering a hacking service, including the ability to hack grades.

2) Misuse of data for purposes detrimental to public education and educators

There are numerous third parties seeking to build databases of teacher and student information. Some are doing so to sell educational software or other products to school districts. Some are collecting information to use for marketing products unrelated to schooling directly to students, teachers, and anyone whose PII they compile. Some are collecting student and teacher PII and nefariously misusing data to tarnish public education and the teaching profession. It appears that this is being done to support privatization, market charter schools, and to reduce the labor costs for education management companies (e.g., CMOs) by undermining the teaching profession, and the job and income security that can help attract and retain educators.

Kate Walsh of the National Council on Teacher Quality recently noted in the *Washington Post* (3/15/15) that the misuse of data on teachers is "a real invasion of privacy." Ms. Walsh was responding to the sort of misuse of teacher and student data associated with the *Los Angeles Times* release of ill-conceived "value-added" ratings for teachers. Such linking of PII on teachers, when connected to students' grades and PII or even simply even classroom-level data, can be misleading, deceptive, and fallacious.

In some cases, third parties are seeking to collect and release information on students and teachers that enables them to publicly release information that "evaluates" a teacher. This is problematic on many fronts, not least of which is the likelihood that such "evaluation" is not valid, slanders a teacher's reputation, and ultimately disrupts the education of students.

Moreover, permitting the release of PII on students and teachers to any third parties, particularly those who may have a privatization or anti-teacher agenda, further cultivates the conditions for misuse and deceptive data reporting. This is ultimately detrimental to the students and teachers in the schools that are subject to such disingenuous reports.

Obliteration of FERPA and deleting parental consent

There have been various federal administrative actions that have weakened protections of student PII, and with it the protections for teachers. The most significant of these changes expands the ability for student data to be shared with third parties without the consent of parents.

Although FERPA requires parental consent for the release of PII, there have always been exclusions, the more extreme of which include third parties under contract with LEAs/SEAs to perform certain educational functions, including research, and to "improve instruction." It is this loophole that has been expanded under the new rules. Prior to 2007, an "authorized representative" under FERPA was undefined and interpretations were very limiting. As a result, data could not be shared with third parties or other state agencies without parental consent, except in very limited cases. Under the revision, "authorized representatives" have been expanded to include third party entities (under contract) and other governmental agencies.

This has resulted in the data equivalent of "loose nukes." Third parties with nefarious intent have been obtaining student and teacher data under the guise of assisting or "auditing" district practices. Some offer their service for free as a means of entry. The likelihood of a breach is huge. The potential for the misuse or spurious use of data is ripe and the ramifications are many.

The expansion of FERPA to allow school data to be shared with other state agencies is also of concern. This was done to pave the way for longitudinal data collection across agencies on matters beyond academic, including "workforce, health, family services, and other data." Under the new rule, SDE could disclose data to, for example, DECD or OPM who could then contract with other third parties to analyze or otherwise manipulate PII.

We urge committee members to add language restoring the strength of FERPA prior to 2008 and to add to this bill provisions for parental and educator consent for the release of PII.

3) Data breaches involving PII occur frequently

The very real concern that student and teacher PII will be breached has only intensified, particularly given recent breaches in more protected industries like health insurance (e.g., Anthem). Stories of student data breaches appear weekly (see examples below), and the vulnerability of student and classroom data linked to individual teachers being breached has increased.

We urge committee members to strengthen data security requirements and to require greater consent for the release of PII on students and educators to limit the dangers of breaches.

For news reports, court cases, analyses of data security issues, CEA recommends the Electronic Data Privacy and Information Center (EPIC) https://epic.org/privacy/student/.

- Emma Brown and Moriah Balingit, Virginia pushed into debate of teacher privacy vs. transparency for parents, Washington Post, March 13, 2015.
- Benjamin Herold, Google Under Fire for Data-Mining Student Email Messages, Education Week, Mar. 13, 2014
- Marc Rotenberg and Khaliah Barnes, Students and Data Privacy, New York Times, May 3, 2014
- Brad Shear, The Student Privacy Bill of Rights, Shear on Social Media Law, Apr. 3, 2014
- Ariel Bogle, What the Failure of inBloom Means for the Student-Data Industry, Slate, Apr. 24, 2014
- Jake Williams, Mining of Student Data Raises Privacy Concerns, FedScoop, May 19, 2014
- The Privacy Guru, Educate Yourself About Student Data Privacy, The Privacy Guru, Apr. 25, 2014
- Bob Unruh, Trouble for Company Collecting Student Data, WND, Apr. 23, 2014
- Ashley Bateman, Louisiana Lawmakers Consider Student Privacy Bill, The Heartland Institute, Apr. 18, 2014
- Anya Kamenetz, What Parents Need To Know About Big Data And Student Privacy, National Public Radio, May 16, 2014
- Khaliah Barnes, Why a 'Student Privacy Bill of Rights' is Desperately Needed, Washington Post, Mar. 6, 2014
- Stacy Khadaroo, Data Breach at Indiana University: Are Colleges Being Targeted, Christian Science Monitor, Feb. 26, 2014
- Benjamin Herold, Education Leaders Tackle Student Data Privacy Issues at Summit, Education Week, Feb. 24, 2014
- Barbara Liston, Florida Lawmakers Push Bills Banning Biometric Scans of School Children, Chicago Tribune, Feb. 4, 2014
- David Nagel, Student Data Not a 'Product' To Be 'Sold to the Highest Bidder', The Journal, Jan. 14, 2014
- Ann Dornfeld, State Deal to Give Media Organizations Student Data Alarms Privacy Experts, KUOW.ORG, Dec. 19, 2013
- Ariel Bogle, Study: Student Data Not Safe in the Cloud, Slate, Dec. 16, 2013
- Molly Hensley-Clancy, U.S. Schools'; Approach to Student Data Threatens Privacy: Study, Reuters, Dec. 13, 2013
- Natasha Singer, Senator Raises Questions About Protecting Student Data, New York Times, Oct. 22, 2013
- Natasha Singer, Group Presses for Safeguards on the Personal Data of Schoolchildren, New York Times, Oct. 13, 2013
- Natasha Singer, Deciding Who Sees Students'; Data, New York Times, Oct. 5, 2013
- Sam Sanders, Students Find Ways to Hack School-Issued iPads Within a Week, Northwest Public Radio, Sept. 27, 2013
- Diane Ravitch, 3 Dubious Uses of Tech in Schools, Salon, Sept. 25, 2013
- David Kravets, Student Suspended for Refusing to Wear RFID Chip Returns to School, Wired, Aug. 22, 2013
- Todd Engdahl, Data Fears Aired Before State Board, ChalkBeat Colorado, May 16, 2013
- Valerie Strauss, Lawsuit Charges Ed Department with Violating Student Privacy Rights, The Washington Post, Mar. 13, 2013

- Chacour Koop, E-number Spreadsheet Leaked, Daily Eastern News, Jan. 23, 2013
- Margo Pierce, The Price of Free Cloud Resources, The Journal, Dec. 4, 2012
- Heather Sells, Big Brother? School District Tracks Kids with RFID, CBN News, October 9, 2012.
- Gazzang, Gazzang Recommends Five Tips to Protect Student Data in the Cloud, September 25, 2012.
- Bailey McGowan, Florida Colleges Ask Court to Revisit FERPA Case Involving Student Who Complained About Professor, Student Press Law Center, September 11, 2012.
- Student Data Will be Given to Military Recruiters, Morning Sentinel, August 22, 2012.
- Mark Boxley, University of Kentucky, Louisville Monitor Athletes' Tweets, USA Today, August 20, 2012.
- Francisco Vara-Orta, Students Will be Tracked via Chips in IDs, San Antonio Express-News, May 26, 2012.

Advertisement for Data Stealing and Abuse
Source: Diane Ravitch 3/17/15

Hackers Scientist, is a professional hacking team based in India. We are prefessioners,we get your work done in less than 48hrs . We are the best in the following:

** HACK AND CHANGE UNIVERSITY GRADES*
** HACK INTO ANY BANK WEBSITE*
** HACK INTO ANY COMPANY WEBSITE*
** HACK INTO ANY GOVERNMENT AGENCY WEBSITE*
** HACK INTO ANY DATA BASE SYSTEM AND GRANT YOU ADMIN PREVELEDGE*
** HACK PAYPAL ACCOUNT*
** Hack WORDPRESS Blogs*
** SERVER CRASHED hack*
** Untraceable Ip etc*
** We can restore LOST FILES AND DOCUMENTS , no matter how long they have been missing*

NOTE
If you refer client to us as a result of the previous job done for you, you will stand a chance of getting any job of your choice hacked for you, free of charge.
We can also teach you how to do the following with our ebook and online tutorials
** Hack and use Credit Card to shop online*
** Monitor any phone and email address*
** Hack Android & iPhones*
** Tap into anybody's call and monitor their conversation*
** Email and Text message interception*

**University grades changing*
**Bank accounts hack*
**Twitters hack*
**email accounts hack*
**Grade Changes hack * load bank account any amounts*
**Website crashed hack*
**server crashed hack*
**Retrieval of lost,gadgets phones , computers and file/documents*
**Erase criminal records hack*
**Databases hack*
**Sales of Dumps cards of all kinds email*